

AAS:JMH  
F.#2017R00878

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

**17M770**

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH:

(1) i\_m\_anonymous@yahoo.com,

THAT IS STORED AT PREMISES  
CONTROLLED BY YAHOO! INC.; AND

(2) jjmgastelum@aol.com

THAT IS STORED AT PREMISES  
CONTROLLED BY AOL, INC.

**TO BE FILED UNDER SEAL**

**APPLICATION FOR  
SEARCH WARRANTS FOR  
INFORMATION IN  
POSSESSION OF A PROVIDER  
(EMAIL ACCOUNT)**

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR SEARCH WARRANTS**

I, JOEL DECAPUA, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for search warrants for information associated with certain email accounts that is stored at premises controlled by Yahoo! Inc. ("Yahoo!"), an email provider headquartered in Sunnyvale, California, and AOL, Inc. ("AOL"), an email provider headquartered in Dulles, Virginia. The information to be searched is described in the following paragraphs and in Attachments A1 (Yahoo!) and A2 (AOL). This affidavit is made in support of an application for search warrants under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo! and AOL to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B1 (Yahoo!) and B2 (AOL). Upon receipt of the

information described in Section I of Attachments B1 and B2, government-authorized persons will review that information to locate the items described in Section II of Attachments B1 and B2.

2. I am a Special Agent with the Federal Bureau of Investigation (“the FBI”), and have been since 2009. I am currently assigned to the Computer Intrusion Squad of the FBI’s New York Division. In my capacity as an FBI Special Agent assigned to the Computer Intrusion Squad, I have participated in numerous investigations involving the use of the Internet in furtherance of criminal activities, including the criminal activities that are at issue in this investigation. I have participated in the execution of numerous search warrants for electronic evidence, including evidence of the type sought by the requested warrants.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1030(a)(7) have been committed by JASON GASTELUM. There is also probable cause to search the information described in Attachments A1 and A2 for evidence, instrumentalities, contraband or fruits of these crimes, as further described in Attachments B1 and B2.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrants because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

**PROBABLE CAUSE**

6. The FBI is investigating a threat communicated via the Internet to St. George's University, an educational institution with offices located in Suffolk County, New York ("the Institution"). The investigation concerns the transmission of threatening communications in interstate or foreign commerce in relation to a protected computer with the intent to extort money or other things of value, by JASON GASTELUM, in violation of 18 U.S.C. § 1030(a)(7), among other offenses.

7. Based on records obtained from the Institution, I know that JASON GASTELUM is a former student of the Institution. In his application for admission, GASTELUM identified his email account as jjmgastelum@aol.com ("the AOL Account"), and listed a residence in Saugus, California as his mailing address ("the Saugus Address"). On or about May 20, 2016, the Institution recommended that GASTELUM be dismissed due to "academic performance" that did "not meet the minimum standards" for the Institution. Records from the Institution also reflect that GASTELUM was dismissed as a student on or about June 8, 2016, and that GASTELUM submitted a letter seeking readmission for the fall semester of 2016 ("the Readmission Letter"). In the Readmission Letter, GASTELUM claimed to have information about an "ongoing epidemic of cheating" that he had observed, which GASTELUM viewed as an "outrage." Based on the Institution's records, I know that GASTELUM was not readmitted as a student at the Institution.

8. On or about April 3, 2017, the Institution received an email message ("the Threat") from an email account with the name of i\_m\_anonymous@yahoo.com ("the Yahoo! Account"). The Threat stated, in sum and substance, that the user of the Yahoo! Account had "hacked" Institution programs and that, if the Institution did not readmit students who had been

“wrongfully dismissed,” that information would be “upload[ed]” to various platforms, including “Facebook pages and DES pages” in an effort to “discredit” the Institution.

9. Based on records obtained from Yahoo! relating to the Yahoo! Account pursuant to subpoena, I know that the Yahoo! Account has been accessed on the following dates and times, from the IP Addresses and ports indicated (“the Target IP Addresses”):

No.	IP Address	Port	Login Time (GMT)	Login Date
1	2605:e000:2487:2500:e9a7:7c23:9063:507e	56952	21:53:57	29-Mar-2017
2	2605:e000:2487:2500:e9a7:7c23:9063:507e	57061	21:53:57	29-Mar-2017
3	2605:e000:2487:2500:8426:c270:3c84:3787	61009	19:17:49	03-Apr-2017
4	172.91.215.142	58554	19:04:47	05-May-2017

10. Based in part on the foregoing information, on June 8, 2017, the government obtained a court order under 18 U.S.C. § 2703(d) directing AOL, Inc. (“AOL”) to identify any subscriber accounts that were accessed from one of the Target IP Addresses during the approximately twenty-four (24) hour period surrounding the instances in which the Yahoo! Account was accessed (“the AOL Order”). The AOL Order was issued by the Honorable A. Kathleen Tomlinson, United States Magistrate Judge for the Eastern District of New York, and was assigned the Miscellaneous Docket Number 17-1660.<sup>1</sup>

---

<sup>1</sup> The government also obtained a similar order under 18 U.S.C. § 2703(d), directed to Yahoo! under Miscellaneous Docket Number 17-1662. Yahoo! responded, in sum and substance, that “A Yahoo ID is required in order to accurately search [Yahoo!’s] system. Therefore, no responsive documents can be produced for the specified [IP] address.”

11. Based on my review of the records provided by AOL in response to the AOL Order, I know that an individual with access to the AOL Account, whom I believe to be GASTELUM, accessed the AOL Account on May 5, 2017, at approximately 18:07:08 (GMT) and 19:52:29 (GMT), from Target IP Address No. 4, i.e., approximately one hour before and 48 minutes after the Yahoo! Account was accessed from Target IP Address No. 4.

12. Also based on my review of the AOL records, I know that the subscriber of the AOL Account is identified as "JASON GASTELUM," with a street address located in Canyon Country, California ("the Canyon Country Address").<sup>2</sup> Based on my review of open source information, I know that the Saugus Address (see ¶ 7, above) is approximately ten minutes, by car, from the Canyon Country Address.

13. Based on the foregoing, I believe that the subscriber to both the Yahoo! Account and the AOL Account is JASON GASTELUM, a former student at the Institution. I also believe that there is probable cause to believe that GASTELUM used the Yahoo! Account to send the Threat to the Institution, and that there is probable cause to believe that evidence relevant to the Threat may be found in the records for both the Yahoo! Account and the AOL Account that are being sought by this application.

14. I also know that preservation requests have been sent to Yahoo! for the Yahoo! Account, and to AOL for the AOL Account. In general, an email that is sent to a Yahoo! or AOL subscriber is stored in the subscriber's "mail box" on the service provider's servers until

---

<sup>2</sup> AOL also identified logins from two other AOL accounts on May 5, 2017, from Target IP Address No. 4. Based on my review of AOL's records and information provided by the Institution, I believe that both accounts belong to individuals who are related to GASTELUM, if not to GASTELUM himself.

the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on the service provider's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on the service provider's servers for a certain period of time.

### **BACKGROUND CONCERNING EMAIL**

15. In my training and experience, I have learned that Yahoo! and AOL provide a variety of on-line services, including electronic mail ("email") access, to the public. Yahoo! and AOL allow subscribers to obtain email accounts at the domain names yahoo.com and aol.com, respectively, like the email accounts listed in Attachments A1 and A2. Subscribers obtain an account by registering with Yahoo! and AOL. During the registration process, Yahoo! and AOL ask subscribers to provide basic personal information. Therefore, the computers of Yahoo! and AOL are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo! and AOL subscribers) and information concerning subscribers and their use of Yahoo! and AOL services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

16. Yahoo! and AOL subscribers can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo! and AOL. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

17. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

18. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

19. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically

retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling investigators to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic



data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

### **CONCLUSION**

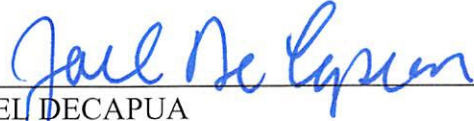
21. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrants will be served on Yahoo! and AOL, respectively, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrants at any time in the day or night.

### **REQUEST FOR SEALING**

22. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, and their attachments, be sealed until November 30, 2017, subject to extension for 90 days upon a showing of continuing need. These documents discuss an ongoing criminal investigation that is neither public nor known to the principal target of the investigation. Accordingly, there is good cause to seal these documents because their

premature disclosure may give that target an opportunity to destroy or tamper with evidence, or otherwise seriously jeopardize the investigation.

Respectfully submitted,



JOEL DECAPUA  
Special Agent  
FBI

Subscribed and sworn to before me on 8/30, 2017

\_\_\_\_\_  
THE HONORABLE JAMES ORENSTEIN  
UNITED STATES MAGISTRATE JUDGE  
EASTERN DISTRICT OF NEW YORK

**ATTACHMENT A1 (Yahoo!)**

**Property to Be Searched**

This warrant applies to information associated with i\_m\_anonymous@yahoo.com, THAT  
IS STORED AT PREMISES CONTROLLED BY YAHOO! INC.; a company that accepts  
service of legal process by email at lawenforcement-request-delivery@yahoo-inc.com.

**ATTACHMENT A2 (AOL)**

**Property to Be Searched**

This warrant applies to information associated with jjmgastelum@aol.com, THAT IS STORED AT PREMISES CONTROLLED BY AOL, INC., a company that accepts service of legal process by email at lawenforcement@teamaol.com.

**ATTACHMENT B1 (Yahoo!)**

**Particular Things to be Seized**

**I. Information to be disclosed by Yahoo! (“the Provider”)**

To the extent that the information described in Attachment A1 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A1, for the period from March 29, 2017, up to and including May 5, 2017:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1030(a)(7), those violations involving JASON GASTELUM and occurring on or after April 3, 2017, including, for each account or identifier listed on Attachment A1, information pertaining to the following matters:

- (a) The transmission, to include both sending and receipt, of any communications to St. George University, an educational institution located in Suffolk County, New York.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

**ATTACHMENT B2****Particular Things to be Seized****I. Information to be disclosed by AOL, Inc. (“the Provider”)**

To the extent that the information described in Attachment A2 is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A2, for the period defined as one hour before and one hour after the dates and times set forth in the following table:

No.	Login Date	Time (GMT)
1	29-Mar-2017	21:53:57
2	29-Mar-2017	21:53:57
3	03-Apr-2017	19:17:49
4	05-May-2017	19:04:47

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates,



account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1030(a)(7), those violations involving JASON GASTELUM and occurring on or after April 3, 2017, including, for each account or identifier listed on Attachment A2, information pertaining to the following matters:

- (a) The transmission, to include both sending and receipt, of any communications to St. George University, an educational institution located in Suffolk County, New York.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).